Customer Scenario:

Company background & information

- Global coffee brand (roastery, wholesale, distribution, retail)
- HQ in Amsterdam. Regional HQs in New York, Dubai, Frankfurt & Singapore
- Warehouses, distribution centres & coffee shops in all these locations
- 100s of other coffee shops in each continent, each lead by their regional HQ
- No operations in China currently
- Strict data sovereignty requirements for all operations in Germany
- Due to COVID-19 looking to migrate all IT workloads to Microsoft Azure
- Currently a typical VMware vSphere estate in each of the regional HQs either in the offices or in co-lo DCs in the same countries, all have a DR DC in the same country too.
- Around 10,000 VMs worldwide
- Due to COVID-19 – heavy investment in online shop/website as main revenue stream for business
    - Developed by teams across the globe – local teams focus on regional specific features/offers/promos
    - Another development team is developing a separate payment service which is subject to PCI-DSS which will be used by the online shop/website
- Global MPLS connecting all sites with regional DC hubs acting as internet breakout points. No local breakouts at each site
- Already utilising Microsoft 365 services (EOL, SharePoint, Teams etc.)

Technical details

- Have a global EA with Microsoft for Microsoft 365 services, Azure consumption & Windows Server/Client licensing (all have active Software Assurance)
- Microsoft 365 Licenses: Office 365 E5 & EM+S E3 for all users
- Azure EA Prepayment (aka Commit): $10 million over 3 years
- Azure Subscriptions: 3 subscriptions in total that developers have been using to test and play in. Can be deleted if required.
- Azure AD Tenant: azurebaristas.onmicrosoft.com
    - Synced with on-premise AD DS Domain: azbaristas.local via Azure AD Connect, Password Hash Sync Enabled & SSO
- Centralised Network team that manages all networking globally with strong skills in the Citrix networking space (ADC, NetScaler etc.)

- All IT staff are trained and certified in Microsoft Azure and have basic to intermediate experience with ARM Templates, Git, GitHub/Azure DevOps.
- A CCoE has been formed between 3 members of each IT team from each regional HQ – total of 12 members – now at 'Ready' phase of CAF

Requirements

- Will go with Azure Native products first approach
- Initial deployment will occur in West Europe
- Needs granular control over Network Resources with a traditional hub and spoke model
- Have agreed to using Azure Landing Zone default policies
- Have agreed to adopt Azure Landing Zone custom role definitions. **However, assignments of these roles will take place in a later stage**
- All Landing Zones Subscriptions must be tagged with the following Tags (at a minimum):
    - Cost-Centre, Environment, IT-Owner-Contact, Service-Application
- Azure Activity Logs for all Subscriptions & Diagnostic settings for all Azure Resources should be enabled automatically and sent to a Log Analytics Workspace. Logs should be kept in there for 180 days.
- Following components will **not** be deployed initially to save cost until first workload will be deployed:
    - DDos Protection Standard
    - Azure Bastion
    - Azure Firewall
    - ExpressRoute Gateway and VPN Gateway
    - Azure Sentinel
- Need to deploy a spoke network and peer it to the hub in order to deploy domain controllers